DIPUTACIÓN DE ALMERÍA

Ingenia
Babel Cybersecurity

INFORME PARA LA FINALIZACIÓN DE LOS CONTRATOS DE OFICINA TÉCNICA

1. Objeto del contrato

El objeto del contrato entre la Diputación de Almería, en adelante DIPALME o Diputación, e Ingenia, se ha centrado en el soporte a la adecuación al Esquema Nacional de Seguridad (ENS) y el Reglamento General de Protección de Datos (RGPD).

En relación al cumplimiento del ENS, el alcance del proyecto ha abarcado los sistemas de información utilizados para la prestación de los diferentes servicios ofrecidos por la Diputación a los ciudadanos, a otras administraciones y a los propios empleados internos en el ejercicio de sus derechos (conforme a la guía CCN-STIC-830- Ámbito de Aplicación del Esquema Nacional de Seguridad).

En relación al RGPD, el alcance del proyecto ha abarcado las personas, procesos, terceros y tecnologías utilizados en el tratamiento de datos personales.

Para más información sobre el objeto y alcance del proyecto, ésta se contiene en la oferta del mismo.

2. Punto de partida

El servicio se ha perfilado como una oficina técnica de soporte para la adecuación de la Diputación al RGPD y al ENS con el siguiente sustrato metodológico:

Aspecto	Herramientas, instrumentos y estándares/requisitos legales	
Requisitos regulatorios de seguridad	En consideración los requisitos del ENS y el RGPD: • ENS: Medidas del Anexo II RD 3/2010 y RD 951/2015 del ENS. • Reglamento Europeo de Protección de Datos (RGPD): (UE)/2016/679.*Neo*LOPD. • Nueva ley orgánica de Protección de Datos (LOPD+gdd): LO 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. • Directiva NIS: Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. • Trasposición de la directiva NIS: Real Decreto–Ley 12/2018.	
Guías de apoyo (CCN y AEPD)	**ENS**	Guías del ENS, serie CCN-STIC-800 e instrucciones técnicas del ENS (Informe del Estado de la Seguridad, Conformidad con el Esquema Nacional de Seguridad y Auditoría)

Aspecto	Herramientas, instrumentos y estándares/requisitos legales	
	RGPD	• Guía para la gestión y notificación de brechas de seguridad. • Protección de Datos: Guía para el Ciudadano • Listado de cumplimiento normativo • Guía del Reglamento General de Protección de Datos para responsables de tratamiento • Guía práctica de análisis de riesgos en los tratamientos • Guía práctica para las Evaluaciones de Impacto • Guía para el cumplimiento del deber de informar • Directrices para la elaboración de contratos entre responsables y encargados de tratamiento • Guía sobre el uso de videocámaras para seguridad y otras finalidades. • Informes de la AEPD
Análisis y Gestión de Riesgos	Se apoya en **MAGERIT** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), junto con la herramienta **PILAR** (Programa Informático Lógico para el Análisis de Riesgos). Esta metodología está alineada con los estándares de análisis y gestión de riesgos ISO 31000 y es una metodología internacionalmente reconocida, por lo que da respuesta a los requisitos de la medida del ENS op.pl.1. Pueden encontrarse detalles de la metodología y la herramienta en el portal http://www.pilar-tools.com/.	
Para los aspectos de la continuidad del servicio	En relación a las medidas de seguridad del ENS relacionadas con la continuidad (op.cont) se tomarán en consideración los siguientes estándares: • ISO 22301:2012 Sistema de Gestión de la Continuidad del Negocio. • ISO 27031 "Tecnología de la información. Técnicas de seguridad. Directrices para la información y la disponibilidad de la tecnología de comunicaciones para la continuidad del negocio".	
Gestión del Proyecto	En la gestión del proyecto se han utilizado los estándares y las buenas prácticas definidas por el **PMI** (Project Management Institute) en su guía **PMBoK**.	
Entrevistas y herramienta de entrevistas	A través de cuestionarios de análisis y auditoría propios de Ingenia, totalmente probados y depurados gracias a la realización de un considerable número de recientes análisis y auditorías de ENS.	
Otras herramientas	Para el cumplimiento técnico y la gestión se usarán herramientas propias del CCN	
Gestión de Cambios	El entorno organizativo del cliente y los requisitos legales externos puede ser susceptible de cambios, por ello se contempla un mecanismo de gestión de cambios, que se basará en re-planificar los trabajos de común acuerdo y continuar trabajando en el nuevo escenario.	
Gestión de la Calidad de los entregables	La documentación será generada conforme a los criterios que se establezcan por la Diputación, en idioma castellano. Se utilizarán los formatos y plantillas que se acuerden en la reunión de inicio. Respecto al **control de calidad de los entregables**, el Director del Proyecto es el responsable último de la supervisión de la calidad de los entregables, antes de que éstos sean emitidos al cliente. Todos los entregables son emitidos en versión borrador, para que el Cliente lo pueda revisar y trasladar a Ingenia los comentarios que considere oportunos. Ingenia resolverá estos comentarios y volverán a emitirse nuevas versiones, que los contemplará, siempre bajo la supervisión del Director de Proyecto. El proceso se podrá repetir hasta alcanzarse una versión definitiva satisfactoria para el Cliente. Si en 15 días desde la emisión de un entregable no se recibiese respuesta, éste se daría por aprobado a todos sus efectos.	
Control y Seguimiento	A través de reuniones periódicas con el cliente (a determinar en el arranque del proyecto) dentro de las actividades de gestión del proyecto	

La filosofía del proyecto ha consistido en abordar los trabajos asociados al cumplimiento de los requisitos regulatorios mencionados anteriormente (ENS, Protección de datos personales) tomando en consideración las diferentes sinergias y coincidencias entre el ENS y la normativa de protección de datos.

3. Actuaciones realizadas y pendientes del plan de mejora y de la hoja de ruta

En el presente inciso del informe se adjuntan las tablas de seguimiento del Plan de Mejora de Seguridad diseñado durante el transcurso del proyecto de adecuación:

- **P01**

PROYECTO /SUBPROYECTO	MEDIDA ENS	HALLAZGO AUDITORÍA 2020	HALLAZGO AUDITORÍA 2021	RESPONSABLE DE LA ACCIÓN	PERSONAL IMPLICADO	INGENIA	DIPALME	REFERENCIA MARCO DOCUMENTAL
P01. Elaboración de Documentación								
P01.01 Normativas y Procedimientos								
P01.01 -1 Flujos de Autorización	ORG.4	OBS-02	NCm-01	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-PROC-20 Procedimiento de Proceso de Autorización
P01.01 -2 Caracterización y Planificación de los Sistemas	OP.PL.3 OP.PL.4	OBS-03 OBS-04	SM-01 NCm-02	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-01 Normativa de Caracterización y Planificación de los Sistemas
P01.01 -3 Adquisición Productos y Sistemas	OP.PL.3	OBS-03	SM-01	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-14 Normativa de Adquisición de Nuevos Sistemas y Productos STIC-PROC-17 Procedimiento de Adquisición de Productos y Servicios TI
P01.01 -4 Control de Accesos y Gestión de Cuentas	OP.ACC.4 OP.ACC.1 OP.ACC.7	NCM-01 OBS-05 OBS-07	NCm-03 NCm-05	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-05 Normativa de Control de Acceso a Sistemas, Redes y Aplicaciones STIC-PROC-07 Procedimiento de Alta, Modificación y Baja de Cuentas de usuario STIC-PROC-10 Procedimiento de Control de Acceso a Redes y Acceso Remoto

PROYECTO /SUBPROYECTO	MEDIDA ENS	HALLAZGO AUDITORÍA 2020	HALLAZGO AUDITORÍA 2021	RESPONSABLE DE LA ACCIÓN	PERSONAL IMPLICADO	INGENIA	DIPALME	REFERENCIA MARCO DOCUMENTAL
P01.01 -5 Evaluación Segregación de Funciones	OP.ACC.3	OBS-06		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-PROC-09 Procedimiento de Evaluación de la segregación de funciones y tareas
P01.01 -6 Procedimiento Gestión Contraseñas	OP.ACC.5	NCm-05	NCm-06	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-PROC-08 Procedimiento de Asignación, Distribución y Almacenamiento de Contraseñas
P01.01 -7 Explotación de Sistemas	OP.EXP.2	OBS-08	NCm-08	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-06 Normativa de Explotación, Operación y Administración de Sistemas
P01.01 -8 Procedimiento Gestión de Vulnerabilidades	OP.EXP.3	OBS-09	NCm-08	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-PROC-13 Procedimiento de Gestión de Vulnerabilidades
P01.01 -9 Procedimiento Gestión de Cambios	OP.EXP.3 OP.EXP.5	OBS-09 OBS-10	NCm-08 NCm-09	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-PROC-12 Procedimiento de Gestión de Cambios y Versiones
P01.01 -10 Prohibición Instalación Aplicaciones	MP.PER.2	NCm-15		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-19 Uso aceptable de activos y medios tecnológicos
P01.01 -11 Protección frente a Código Dañino	OP.EXP.6	OBS-11		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del	Realizado	Realizado	STIC-PROC-14 Procedimiento de Protección frente a Código Dañino

PROYECTO /SUBPROYECTO	MEDIDA ENS	HALLAZGO AUDITORÍA 2020	HALLAZGO AUDITORÍA 2021	RESPONSABLE DE LA ACCIÓN	PERSONAL IMPLICADO	INGENIA	DIPALME	REFERENCIA MARCO DOCUMENTAL
					Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías			
P01.01 -12 Gestión de Ciberincidentes	OP.EXP.7	NCM-03	NCm-10	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-16 Normativa de Gestión de Incidentes STIC-PROC-11 Procedimiento de Gestión de Incidentes
P01.01 -13 Controles Criptográficos	OP.EXP.11	OBS-12	SM-04	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-21 Normativa de Controles Criptográficos
P01.01 -14 Normativa Seguridad Física	MP.IF.1	OBS-13		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-04 Normativa de Seguridad Física STIC-PROC-05 Procedimiento de Control de Acceso Físico al CPD STIC-PROC-06 Procedimiento de Acceso a los Edificios STIC-PROC-23 Procedimiento de Entrada y Salida de Equipamiento
P01.01 -15 Normativa Seguridad en RRHH	MP.PER.1	NCm-14	SM-06	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-03 Normativa sobre el Personal y los Recursos Humanos
P01.01 -16 Buen Uso de Medios Tecnológicos	MP.PER.2	NCm-15		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-19 Uso aceptable de activos y medios tecnológicos STIC-PROC-04 Procedimiento de Uso de Memorias Extraíbles
P01.01 -17 Normativa Formación y Concienciación	MP.PER.3 MP.PER.4	NCm-16 NCm-17	SM-07	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del	Realizado	Realizado	STIC-PROC-24 Procedimiento de Formación y Concienciación en materia de Seguridad

PROYECTO /SUBPROYECTO	MEDIDA ENS	HALLAZGO AUDITORÍA 2020	HALLAZGO AUDITORÍA 2021	RESPONSABLE DE LA ACCIÓN	PERSONAL IMPLICADO	INGENIA	DIPALME	REFERENCIA MARCO DOCUMENTAL
					Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías			
P01.01 -18 Política de Mesas Limpias	MP.EQ.1	OBS-14		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-19 Uso aceptable de activos y medios tecnológicos
P01.01 -19 Normativa Uso de Equipos Portátiles	MP.EQ.3	OBS-15		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-20 Normativa de Protección de Equipos Portátiles
P01.01 -20 Normativa Seguridad en la Red	MP.COM.1	OBS-16		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-07 Normativa de Seguridad de la Red STIC-PROC-10 Procedimiento de Control de Acceso a Redes y Acceso Remoto
P01.01 -21 Normativa Gestión de Soportes	MP.SI.1 MP.SI.4 MP.SI.5	OBS-18 OBS-19 OBS-20	OBS-03	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-09 Normativa de Gestión de Soportes STIC-PROC-02 Procedimiento de Gestión de Soportes STIC-PROC-03 Procedimiento de Baja de Soportes
P01.01 -22 Seguridad Aplicaciones y SW	MP.SW.1	OBS-21		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-15 Normativa de Seguridad de Aplicaciones y Software STIC-PROC-19 Procedimiento de Gestión del Software
P01.01 -23 Normativa Clasificación de la Información	MP.INFO.2	OBS-23	NCm-15	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-02 Normativa de Clasificación de la Información STIC-PROC-01 Procedimiento de Etiquetado y Clasificación de la Información

PROYECTO /SUBPROYECTO	MEDIDA ENS	HALLAZGO AUDITORÍA 2020	HALLAZGO AUDITORÍA 2021	RESPONSABLE DE LA ACCIÓN	PERSONAL IMPLICADO	INGENIA	DIPALME	REFERENCIA MARCO DOCUMENTAL
P01.01 -24 Política de Firma Electrónica	MP.INFO.4	X		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	N/A	Realizado	Se ha publicado y aprobado la Política de Firma Electrónica, por resolución de presidencia, BOP 26/08/2020 (Resolución nº 2069 de fecha 3 de agosto de 2020)
P01.01 -25 Publicación Web y Gestión Metadatos	MP.INFO.6	NCm-20	NCm-16	RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-PROC-18 Procedimiento de Limpieza de Documentos
P01.01 -26 Copias de Seguridad y Restaurado	MP.INFO.9	OBS-24		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-08 Normativa de Copias de Seguridad STIC-PROC-15 Procedimiento de Copias de Seguridad STIC-PROC-16 Procedimiento de Restaurado Información
P01.01 -27 Normativa Uso Correo Electrónico	MP.S.1	OBS-25		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-13 Normativa de protección del correo electrónico
P01.01 -28 Protección Servicios Expuestos a Internet	MP.S.2	OBS-26		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-12 Normativa de protección de los servicios expuestos a internet
P01.01 -29 Actuación ante Ataques DoS	MP.S.8	OBS-27		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-PROC-21 Procedimiento de Prevención DDoS
P01.01 -30 Teletrabajo	MP.PER.2	X		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del	Realizado	Realizado	STIC-PROC-26 Procedimiento de Teletrabajo

PROYECTO /SUBPROYECTO	MEDIDA ENS	HALLAZGO AUDITORÍA 2020	HALLAZGO AUDITORÍA 2021	RESPONSABLE DE LA ACCIÓN	PERSONAL IMPLICADO	INGENIA	DIPALME	REFERENCIA MARCO DOCUMENTAL
					Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías			
P01.02 Documentación Técnica								
P01.02 -1 Descripción Técnica Instalaciones	OP.PL.2	NCm-03		RESPONSABLE DEL SISTEMA	Equipo de Servicio de Nuevas Tecnologías	N/A	Realizado	Se está generando la documentación.
P01.03 Terceros								
P01.03 -1 Normativa de Contratación	OP.EXT.1	NCm-08		RESPONSABLE DE SEGURIDAD	Responsable de Seguridad, Responsable del Sistema, Equipo del Servicio de Organización, Equipo de Servicio de Nuevas Tecnologías	Realizado	Realizado	STIC-NOR-18 Normativa Contratación y Relaciones con Terceros STIC-PROC-22 Procedimiento de Contratación y Relaciones con Terceros

- **P02**

PROYECTO /SUBPROYECTO	ESTADO	DESCRIPCIÓN	MEDIDA ENS	APLICA A NIVEL SEGURIDAD	HALLAZGO AUDITORÍA 2020	HALLAZGO AUDITORÍA 2021	RESPONSABLE
P02. Actuaciones Organizativas y Operativas							
P02.01 Marco Normativo							
P02.01 -1 Aprobar Política de Seguridad	FINALIZADO	Diputación de Almería debe formalizar la designación de un nuevo responsable de seguridad tras la jubilación del anterior responsable	ORG.1	BASICO	OBS01		RESPONSABLE DE SEGURIDAD
P02.01 -2 Redactar y Aprobar Normativas	FINALIZADO	Redactar, revisar y aprobar Normativas de Seguridad	ORG.2	BASICO	NCm01		RESPONSABLE DE SEGURIDAD
P02.01 -3 Redactar y Aprobar Procedimientos	FINALIZADO	Redactar, revisar y aprobar procedimientos de seguridad	ORG.3	BASICO	NCm02		RESPONSABLE DE SEGURIDAD
P02.02 Planificación Seguridad							
P02.02 -1 Análisis de Riesgos	FINALIZADO	Se debe revisar y actualizar (si fuera necesario) el análisis de riesgos de forma anual, o cuando se produzcan cambios relevantes en los sistemas de información.	OP.PL.1	BASICO +	X		RESPONSABLE DE SEGURIDAD
P02.02 -2 Sistema de Gestión de la Seguridad	FINALIZADO	Implantar un sistema de gestión de la seguridad, que comprenda la planificación, organización y control de todos los elementos del sistema de información	OP.PL.2	BASICO +	X		RESPONSABLE DE SEGURIDAD
P02.02 -3 Soporte Técnico y Mantenimiento	FINALIZADO	Todos los sistemas de información deberán contar con el correspondiente soporte técnico y mantenimiento que permita minimizar las vulnerabilidades de seguridad y mantener los equipos y sistemas correctamente actualizados	OP.EXP.4	BASICO	NCm-06	SM-03	RESPONSABLE DE SEGURIDAD SERVICIO DE NUEVAS TECNOLOGÍAS
P02.02 -4 Revisión Registros Auditoría	PENDIENTE	Revisión de los registros de auditoría para la detección de patrones anómalos	OP.EXP.8	BASICO +	NCm-07	NCm-11	SERVICIO DE NUEVAS TECNOLOGÍAS
P02.02 -5 Análisis de Impacto en el Negocio (BIA)	FINALIZADO	Se deberá realizar un análisis de impacto en el negocio (BIA) en los sistemas categorizados como de nivel MEDIO en el ENS	OP.CONT.1	MEDIO	NCm-10		RESPONSABLE DE SEGURIDAD SERVICIO DE NUEVAS TECNOLOGÍAS
P02.02 -6 Mediciones Informes INES	FINALIZADO	Realización del Informes INES. Se deberán recopilar todos los datos exigidos en el Informes INES relacionados con seguridad de la información, y con el histórico anual del sistema de gestión de incidentes	OP.MON.2	BASICO +	X	SM-05	RESPONSABLE DE SEGURIDAD SERVICIO DE NUEVAS TECNOLOGÍAS
P02.02 -7 Registro Entradas y Salidas en Inventario	PENDIENTE	A través del sistema implantado para gestión del inventario de elementos del sistema de información, se deberán registrar las actuaciones para cada uno de los	MP.IF.7	BASICO	NCm-13		SERVICIO DE NUEVAS TECNOLOGÍAS

PROYECTO /SUBPROYECTO	ESTADO	DESCRIPCIÓN	MEDIDA ENS	APLICA A NIVEL SEGURIDAD	HALLAZGO AUDITORÍA 2020	HALLAZGO AUDITORÍA 2021	RESPONSABLE
		elementos, incluyendo los registros de las entradas y salidas de equipamiento (PCs, Servidores, Elementos HW de Red, Portátiles, etc.)					
P02.02 -8 Adecuación RGPD y LOPDgdd	FINALIZADO	Finalizar el plan de adecuación al RGPD y acometer todas las medidas jurídicas del plan de mejora de la seguridad. Se asocia a las medias P04 del Plan de Mejora	MP.INFO.1	BASICO	OBS-23	SM-08	RESPONSABLE DE SEGURIDAD
P02.03 Recursos Humanos							
P02.03 -1 Requisitos Medios Humanos	FINALIZADO	Se deberán tener en cuenta las necesidades de personal, y su cualificación y formación necesaria en materia de seguridad, a la hora de un nuevo proyecto TI (nuevo aplicativo, nuevo sistema de información, nuevo servicio TI, etc.).	OP.PL.4	MEDIO	X	NCm-02	ÁREA RRHH RESPONSABLE DE SEGURIDAD
P02.03 -2 Caracterización Puestos de Trabajo	FINALIZADO	Caracterización de cada puesto de trabajo en materia de seguridad, incluyendo al menos, responsabilidades, cualificación y capacitación en materia de seguridad	MP.PER.1	MEDIO	NCm-14	SM-06	ÁREA RRHH RESPONSABLE DE SEGURIDAD
P02.03 -3 Deberes y Obligaciones del Personal	PENDIENTE	El personal de Diputación deberá firmar un documento de deberes y obligaciones en materia de seguridad	MP.PER.2	BASICO	NCm-15		ÁREA RRHH RESPONSABLE DE SEGURIDAD
P02.04 Terceros							
P02.04 -1 Requisitos de Seguridad en Contratos	PENDIENTE	Los contratos realizados de forma no centralizada, desde cada área/servicio, deberán incluir los aspectos y requisitos seguridad necesarios relativos a seguridad de la información y protección de datos personales	OP.EXT.1	MEDIO	NCm-08		RESPONSABLE DE SEGURIDAD
P02.04 -2 Compromiso Seguridad Ayuntamientos	PENDIENTE	En los convenios con Ayuntamientos se debe indicar que los Ayuntamientos deberán disponer de las medidas de seguridad físicas suficientes para asegurar la protección de los datos personales que almacenan en sus instalaciones, relacionados con los trabajos de personal de Diputación en dichos Ayuntamientos.	OP.EXT.1	MEDIO	NCm-08		RESPONSABLE DE SEGURIDAD
P02.04 -3 Listado Proveedores	PENDIENTE	Elaborar un listado de proveedores, con todos los datos necesarios que pudieran hacer falta en caso de incidencia relacionada con seguridad de la información. Se debe disponer de forma centralizada de toda la información sobre el contrato, vigencia, condiciones de mantenimiento para cada proveedor, contacto en caso de incidencia y SLA, etc.	OP.EXT.2	MEDIO	NCm-09	NCm-12	RESPONSABLE DE SEGURIDAD SERVICIO DE NUEVAS TECNOLOGÍAS
P02.04 -4 Informe Seguimiento Terceros	PENDIENTE	Se debe realizar seguimiento al tercero, para la evaluación del proveedor en cuanto al cumplimiento de requisitos relacionados con seguridad de la información.	OP.EXT.2	MEDIO	NCm-09	NCm-12	RESPONSABLE DE SEGURIDAD SERVICIO DE NUEVAS TECNOLOGÍAS

PROYECTO /SUBPROYECTO	ESTADO	DESCRIPCIÓN	MEDIDA ENS	APLICA A NIVEL SEGURIDAD	HALLAZGO AUDITORÍA 2020	HALLAZGO AUDITORÍA 2021	RESPONSABLE
P02.05 Seguridad Física							
P02.05 -1 Identificación y Acreditación Visitas	X	Se deberá identificar y acreditar a los visitantes que acceden al edificio principal de Diputación (donde se ubica el CPD principal), y al edificio ubicado en Rambla Alfareros, donde se ubica el CPD secundario.	X	X	SM-01		X
P02.05 -2 Listado Autorizados Acceso CPDs	PENDIENTE	Se debe disponer de un listado de personal autorizado a acceder a ambos CPD, principal y secundario, supervisado y revisado por el Responsable de Seguridad.	MP.IF.2	BASICO	NCm-11	OBS-01	SERVICIO DE NUEVAS TECNOLOGÍAS
P02.05 -3 Registro Accesos CPDs	PENDIENTE	Se deben registrar los accesos a ambos CPD. El Responsable de Seguridad debe revisar de forma periódica los registros para detección de accesos no autorizados	MP.IF.2	BASICO	NCm-11	OBS-01	SERVICIO DE NUEVAS TECNOLOGÍAS
P02.05 -4 Almacenamiento Información en Papel	FINALIZADO	Todas las áreas de Diputación deben disponer de armarios suficientes para almacenar la documentación de trabajo diario e intermedia (previa a Archivo) de forma adecuada y con los mecanismos adecuados que permitan almacenar la información de forma segura	MP.SI.3	BASICO	NCm-18		RESPONSABLE DE SEGURIDAD
P02.05 -5 Destructoras de Papel	FINALIZADO	Identificar las áreas de Diputación que no cuentan con destructora de papel. Ya sea de forma centralizada, o específicamente desde dichas áreas, se deberá proceder a la implantación de destructora de papel en las áreas que no disponen de ella (o que la destructora más cercada se encuentra demasiado alejadas de la zona de trabajo).	MP.SI.5	BASICO +	OBS-21	OBS-03	RESPONSABLE DE SEGURIDAD
P02.06 Formación y Concienciación							
P02.06 -1 Acciones Concienciación	FINALIZADO	Plan de Concienciación	MP.PER.3	BASICO	NCm-16	SM-07	RESPONSABLE DE SEGURIDAD
P02.06 -2 Acciones Formativas	FINALIZADO	Plan de Formación	MP.PER.4	BASICO	NCm-17	SM-07	RESPONSABLE DE SEGURIDAD

- **P03**

ACCIÓN	DENOMINACIÓN	ESTADO	TAREAS	RESPONSABLE	MEDIDA ENS	APLICA A NIVEL SEGURIDAD	HALLAZGO AUDITORÍA 2020	HALLAZGO AUDITORÍA 2021
P03.01 -1	Revisión Periódica Cuentas de Usuario	PENDIENTE	Se debe realizar una revisión periódica de las cuentas de usuario, para verificar y eliminar las cuentas de usuarios dados de baja, y eliminar accesos de usuarios que hayan cambiado su rol, o puesto de trabajo y sigan manteniendo acceso a aplicaciones que ya no utilicen, todo en base a las normativa de control de acceso y el procedimiento de alta, baja y modificación de cuentas de usuario	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.ACC.4	BASICO =	NCM-01	NCm-05
P03.01 -2	Doble Factor de Autenticación	PENDIENTE	Implantar doble factor de autenticación en las aplicaciones y sistemas que así lo requieran: - Aplicativos y sistemas de categoría MEDIA en el ENS - Aplicativos y sistemas que operen con datos personales de categoría especial	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.ACC.5	BASICO +	NCm-04	NCm-06 SM-02
P03.01 -3	Requisitos Contraseñas	PENDIENTE	Verificar que todas las aplicaciones cumplen con los requisitos de fortaleza de contraseñas definidos en las normas y procedimientos asociados, así como con los requisitos de periodicidad de cambio.	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.ACC.5	BASICO +	NCm-04	NCm-06
P03.01 -4	Bloqueo Intentos Fallidos Acceso	PENDIENTE	Se debe bloquear al usuario tras varios intentos fallidos de acceso consecutivos. El número de intentos deberá estar definido en las normativas de control de acceso y políticas sobre uso seguro de contraseñas	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.ACC.6	BASICO +	NCM-02	NCm-07
P03.01 -5	Información Últimos Accesos	PENDIENTE	Para los Sistemas de categoría MEDIA en el ENS, se deberá mostrar información sobre fecha y hora del último o últimos accesos, así como información sobre los intentos fallidos de acceso	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.ACC.6	BASICO +	NCM-02	NCm-07
P03.01 -6	Registro de Accesos	PENDIENTE	Se deberán registrar los accesos con éxito y los accesos fallidos a los diferentes sistemas de información	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.ACC.6	BASICO +	NCM-02	NCm-07
P03.01 -7	Diálogos de Acceso	PENDIENTE	Los diálogos de acceso a los Sistemas de la Diputación deben prevenir sobre el acceso y el correcto uso de los mismos y las obligaciones del usuario. Así mismo, no deben revelar información confidencial, únicamente la indispensable.	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.ACC.6	BASICO +	NCM-02	NCm-07
P03.01 -8	Contraseñas por defecto	FINALIZADO	Se deben retirar las contraseñas por defecto de todos los dispositivos de red.	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.EXP.2	BASICO	OBS-08	NCm-08
P03.02 -1	App Inventario de Activos	PENDIENTE	Se dispondrá de un inventario de activos de información permanentemente actualizado, en el que se identifique la ubicación, el responsable de cada activo, y los diferentes cambios y actuaciones sobre los mismos. Deberá comprender, al menos: - Aplicaciones SW - Equipos HW - Dispositivos de Red - Dispositivos Móviles Corporativos - Equipos Portátiles - Soportes en su caso (memorias extraíbles) - Relación de personal, que permita asignar responsables de los diferentes sistemas de información o usuarios que interaccionen con los mismos.	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.EXP.1	BASICO	NCm-05	OBS-02

ACCIÓN	DENOMINACIÓN	ESTADO	TAREAS	RESPONSABLE	MEDIDA ENS	APLICA A NIVEL SEGURIDAD	HALLAZGO AUDITORÍA 2020	HALLAZGO AUDITORÍA 2021
P03.02 -2	App Herramienta Anti-Malware	FINALIZADO	Se dispondrá de una herramienta anti malware contra código dañino, capaz de detectar diferentes tipos de malware y actuar según el caso. - BBDD de malware actualizada regularmente - Revisión de cada aplicación al arranque - Bloqueo de acceso a sitios web maliciosos (black lists) - Revisión de los archivos adjuntos recibidos y descargados relativos al sistema de correo electrónico - Comprobación de existencia de malware desde diferentes puntos de la red	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.EXP.6	BASICO	OBS-11	
P03.02 -3	App Gestión de Incidencias	PENDIENTE	Implantación de herramienta para el registro y la gestión y seguimiento de incidentes de seguridad de la información	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.EXP.7 OP.EXP.9	MEDIO	NCM-03 NCM-04	NCm-10 NCm-10
P03.02 -4	App Archivo Electrónico	PENDIENTE	Implantación de un archivo electrónico	SERVICIO DE NUEVAS TECNOLOGÍAS	MP.SI.3	BASICO	NCm-18	
P03.02 -5	App Escaneo de Vulnerabilidades	PENDIENTE	Se deberá disponer de una herramienta para la identificación de vulnerabilidades	SERVICIO DE NUEVAS TECNOLOGÍAS	MP.SW.2	BASICO +	NCm-19	NCm-14
P03.02 -6	App Gestión Metadatos	PENDIENTE	Utilizar herramientas para la gestión de metadatos	SERVICIO DE NUEVAS TECNOLOGÍAS	MP.INFO.6	BASICO	NCm-20	NCm-16
P03.03 -1	Revisión Principios Privilegios Mínimos	FINALIZADO	Las contraseñas de acceso a los servidores deben ser conocidas únicamente por los usuarios que lo necesiten para el desempeño de sus funciones (revisión regla de funcionalidad y privilegios mínimos)	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.EXP.2	BASICO	OBS-08	NCm-08
P03.03 -2	Usuarios como Administradores	PENDIENTE	Se recomienda que los usuarios no sean administradores de sus propias máquinas, y que así se refleje en las diferentes políticas y normativas relacionadas con el control de acceso a los sistemas de información y la asignación de privilegios	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.EXP.2	BASICO	OBS-08	NCm-08
P03.04 -1	Migración Sistemas sin Soporte	PENDIENTE	Se deberá realizar la migración de aplicaciones de sistemas sin soporte técnico, tipo Windows XP	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.EXP.4	BASICO	NCm-06	SM-03
P03.04 -2	Pentesting y Auditorías Hacking Ético	PENDIENTE	Realización periódica de pruebas de pen-testing para la identificación de vulnerabilidades	SERVICIO DE NUEVAS TECNOLOGÍAS	MP.SW.2	BASICO +	NCm-19	NCm-14
P03.04 -3	Identificación de Vulnerabilidades	PENDIENTE	Identificación de vulnerabilidades de forma previa al paso a producción (categoría media ENS)	SERVICIO DE NUEVAS TECNOLOGÍAS	MP.SW.2	BASICO +	NCm-19	NCm-14
P03.04 -4	Uso de Protocolo Seguro HTTPS	FINALIZADO	Utilización de HTTPS en todas las páginas Web de Diputación. La página principal corporativa de Diputación no dispone de HTTPS.	SERVICIO DE NUEVAS TECNOLOGÍAS	MP.S.2	BASICO	NCm-21	
P03.05 -1	Sondas Equipos CERT	FINALIZADO	Conexión mediante sondas a CERTS a nivel autonómico/estatal (equipos de respuesta ante incidentes)	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.EXP.7	MEDIO	NCM-03	NCm-10
P03.05 -2	Activación Registros de Auditoría	PENDIENTE	Activación de los registros de auditoría en los servidores y aplicaciones críticas para propiciar la trazabilidad de la información en todos los casos	SERVICIO DE NUEVAS TECNOLOGÍAS	OP.EXP.8	MEDIO	NCm-07	NCm-11
P03.05 -3	Cifrado de Soportes	PENDIENTE	Análisis de necesidad de cifrado de soportes de información en función de la información contenida (sensibilidad, confidencialidad, criticidad), e implantación de las medidas criptográficas que se determinen.	SERVICIO DE NUEVAS TECNOLOGÍAS	MP.SI.2	MEDIO	OBS-19	

ACCIÓN	DENOMINACIÓN	ESTADO	TAREAS	RESPONSABLE	MEDIDA ENS	APLICA A NIVEL SEGURIDAD	HALLAZGO AUDITORÍA 2020	HALLAZGO AUDITORÍA 2021
P03.05 -4	Seguridad	FINALIZADO	Se debe asegurar la autenticación del otro extremo del canal antes de intercambiar información alguna. Además, se deben utilizar de mecanismos para la prevención de ataques activos (alteración de la información en tránsito, inyección de información espuria, secuestro de la sesión por terceras partes, etc.) en todos los canales de comunicación utilizados y, en caso de ocurrir, su detección con la consiguiente activación de los procedimientos previstos de tratamiento del incidente	SERVICIO DE NUEVAS TECNOLOGÍAS	MP.COM.3	BASICO +	OBS-17	
P03.06 -1	Sistema de Control de Accesos	PENDIENTE	Implantación de un sistema de control de accesos al edificio principal de Diputación (donde se ubica el CPD principal), y al edificio ubicado en Rambla Alfareros, donde se ubica el CPD secundario.	SERVICIO DE NUEVAS TECNOLOGÍAS	MP.IF.1	BASICO	OBS-13 SM-01	OBS-01
P03.06 -2	Medidas Contra Inundación CPD Sec	PENDIENTE	Implantación de medias contra inundación en el CPD de Rambla Alfareros (CPD Secundario)	SERVICIO DE NUEVAS TECNOLOGÍAS	MP.IF.6	MEDIO	NCm-12	
P03.04 -5	Mantenimiento listado de sw autorizado	PENDIENTE	Se debe proceder a elaborar el listado de Software Autorizado de Diputación	SERVICIO DE NUEVAS TECNOLOGÍAS	MP.SW.1	BASICO +	NCm-19	

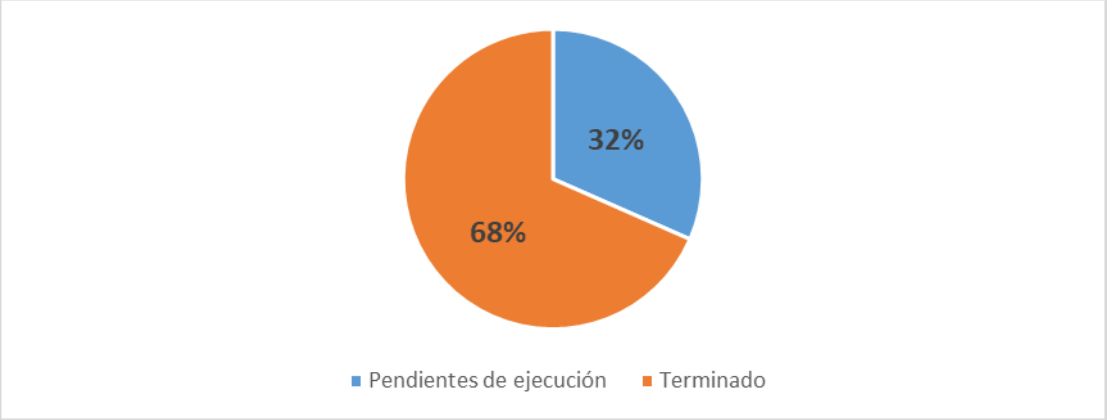
- **P.04**

ACCIÓN	DENOMINACIÓN	ESTADO	TAREAS
P04.01 Procedimientos Jurídicos			
P04.01 -1	P04.01 -1 Manual Jurídico	FINALIZADO	Redactar y aprobar un manual de procedimientos jurídicos, que disponga todas las actuaciones en materia de protección de datos personales por parte de Diputación.
P04.01 -2	P04.01 -2 Proceso de Revisión RAT	FINALIZADO	Las diferentes áreas de Diputación deben revisar los tratamientos que les competen, así como la información contenida en el RAT: - Bases Jurídicas. Se debe señalar en el RAT las normativas asociadas en caso de competencia de la Diputación, o cumplimiento de una Ley - Finalidades - Destinatarios (cesiones) - Encargos de Tratamiento - Datos tratados - Datos de categoría especial - Plazos de conservación Se deben modificar algunas base legítimas basadas en el consentimiento, ya que se ha analizado y establecido que la base jurídica que aplicaría por ser AAPP sería otra (competencias propias de la AAPP; cumplimiento de una Ley; Interés Público). En las entrevistas realizadas a las Áreas en octubre19 se han identificado algunos de los cambios y revisiones específicas necesarias que se deben acometer desde cada área, incluyendo en algunos casos la necesidad de aglutinar tratamientos, modificar alguno de los existentes, o ampliar con algún tratamiento nuevo. No obstante, los responsable de área deberán revisar el RAT de forma periódica.
P04.01 -3	P04.01 -3 Procedimiento Ejercicio Derechos	FINALIZADO	Redactar procedimiento relativo al ejercicio de derechos RGPD/LOPDgdd, así como las plantillas necesarias para la solicitud de ejercicio de derechos, la comunicación desde cualquier área al DPD, así como las contestaciones al ciudadano y comunicados/resoluciones posibles para cada derecho. En las cláusulas de deber de información estarán previstas las diferentes vías para el ejercicio de derechos: en persona, a través de mail, a través de sede electrónica (procedimiento genérico, o procedimiento específico cuando exista). Se deberán publicar los PDF en Internet con los modelos de solicitudes para que el ciudadano pueda descargarlos, firmarlos y enviarlos por mail o en persona si así lo decidiera.
P04.02 -4	P04.01 -4 Procedimiento ante Brechas de Seguridad	FINALIZADO	Incluir en el procedimiento de gestión de ciber incidentes la necesidad de notificación a AEPD en caso de incidencia y necesidad de comunicación a los afectados en su caso.
P04.02 Cláusulas			
P04.02-1	P04.02 -1 Cláusulas Deber de Información	FINALIZADO	Añadir las cláusulas a todos los formularios en papel, impresos, formularios Web, y demás sitios donde se recaban datos personales, en caso de que no se disponga de cláusulas de tratamiento de datos, o estén desactualizadas (LOPD1999). Las cláusulas deben cumplir con el deber de información.
P04.03 Medidas Técnicas			
P04.03 -1	P04.03 -1 Seguridad desde el Diseño	FINALIZADO	Antes de cualquier tratamiento nuevo de datos personales, se deberá realizar un análisis de los principales riesgos y medidas a adoptar para que el tratamiento pueda realizarse de forma segura. Este análisis debe hacerse de forma previa a la realización de la actividad de tratamiento (fase de diseño).
P04.03 -2	P04.03 -2 Medidas Jurídicas y ENS - AR PILAR	FINALIZADO	Finalizar el plan de adecuación al RGPD y acometer todas las medidas jurídicas del plan de mejora de la seguridad, y las medidas del ENS asociadas.
P04.03 -3	P04.03 -3 Análisis de Riesgos Tratamientos	FINALIZADO	Se realizará el análisis de riesgos de cada tratamiento, realizando primero una evaluación de necesidad (o no) de EIPD

ACCIÓN	DENOMINACIÓN	ESTADO	TAREAS
P04.03 -4	P04.03 -4 Evaluación de Impacto	FINALIZADO	Se deberá realizar un análisis de riesgos y evaluación del impacto en la protección de datos, para nuevos tratamientos en los que exista necesidad de EIPD en base a los criterios de las diferentes guías sobre evaluación de impacto de la AEPD y demás organismos autonómicos autorizados.
P04.04 Organizativas			
P04.04 -1	P04.04 -1 Diputación como Co-Responsable	FINALIZADO	Definir los casos en los que Diputación pudiera ser corresponsable de tratamiento
P04.04 -2	P04.04 -2 Inventario Encargados de Tratamiento	FINALIZADO	Diputación debe disponer de un inventario de encargados de tratamiento, en el que se indique al menos: - tratamiento asociado y área que lo gestiona - vigencia del contrato - si han firmado o no las cláusulas de encargo de tratamiento - persona de contacto ante cualquier incidente seguridad - medidas de seguridad que se deban aplicar Durante las entrevistas a las diferentes áreas realizadas en Octubre19, se han identificado encargados de tratamiento. No obstante, el inventario de ET debe revisarse por los responsables de área de forma periódica.
P04.04 -3	P04.04 -3 Diputación como Encargada del Tratamiento	FINALIZADO	Se debe decidir si en las asistencias a municipios y otros tratamiento similares, Diputación sería encargada o responsable del tratamiento.

4. Objetivos conseguidos

De las acciones contenidas en la hoja de ruta expuesta en el punto 3 del informe, un 68% de las acciones se encuentran en estado “Finalizadas”.



5. Evaluación del proyecto

De la relación de proyectos incluidos en el Plan de Mejora de la Seguridad de la Diputación de Almería, que forman parte del análisis de riesgos con alcance del Esquema Nacional de Seguridad (ENS) y los artículos del Reglamento general de Protección de Datos (RGPD), el 68 % de las acciones propuestas se han llegado a finalizar o, en su caso, dotar de suficiente iteración, al tener matices de recurrencia.

Previamente a la proposición del plan de mejora y sus respectivos proyectos de acciones se realizó un Análisis de Riesgos de Seguridad de la Información que ha permitido identificar dónde residen los mayores riesgos para las actividades relacionadas con las tecnologías de la información y el tratamiento de datos personales, que puedan afectar a la actividad de la Diputación.

Para mitigar los riesgos identificados, así como cumplir con los requisitos de las medidas de seguridad incluidas en el Anexo II del ENS, y con los artículos del RGPD, la consecución de la relación de acciones propuestas permitiría situar a la Diputación, en relación a su mapa de riesgos, por debajo del nivel de riesgo aceptable definido en los diferentes informes relacionados con la adecuación al ENS.

En la fase de implementación y seguimiento del proyecto de acciones para la adecuación, tanto Ingenia como los diferentes miembros de la Diputación de Almería con responsabilidades en el ENS y el RGPD , de manera conjunta y colaborativa, a través de seguimientos periódicos han conseguido ir implementando las acciones sugeridas o en-

contrando soluciones alternativas o interpretaciones a la acción para ir, progresivamente, subiendo el nivel de cumplimiento de la Diputación respecto a las normas citadas.

Es de destacar la profesionalidad, rigor, buen hacer y calidad humana del equipo de trabajo de la Diputación de cara a conseguir, en la medida de lo posible, los objetivos propuestos.

No obstante, se ha de tener en cuenta las circunstancias comunes a la gran mayoría de entes de la administración pública en relación a la carga de trabajo en sus funciones y obligaciones para con la ciudadanía para matizar y dar como satisfactorio un grado de avance en el plan como el que se resumen en este informe y se detalla en los diferentes entregables e informes de seguimiento realizados durante el transcurso del proyecto.

6. Propuestas de mejora y conclusión

A modo de resumen, se enuncian propuestas de línea de mejora para la progresiva iteración en el cumplimiento del ENS y RGPD:

- Continuar con la periodicidad en realización de sesiones de trabajo con el objetivo de seguir la hoja de ruta de los diferentes proyectos de acciones del Plan de mejora de la seguridad.
- Tener en cuenta las conclusiones de la última auditoría ENS realizada.
- Continuar con los trabajos de mejora en el ámbito del RGPD y la actualización del aplicativo Prodatos, siguiendo la metodología utilizada en los últimos meses.
- Priorizar el cumplimiento en el RD 3/2010 del Esquema Nacional de Seguridad sin perder de vista las modificaciones introducidas en el RD 311/2022 para configurar a futuro las adaptaciones que sean necesarias.
- Calendarizar y optimizar las sesiones de trabajo de los equipos internos de Diputación que se encarguen de la implementación progresiva de las acciones pendientes de finalizar.